REMARKS

The Applicants and the undersigned thank Examiner Ha for her careful review of this application. Claims 1-9 and 11-65 have been rejected. Upon entry of this amendment, Claims 1-9 and 11-65 remain pending in this application. Claim 10 has been cancelled without prejudice to or disclaimer of the subject matter contained therein.

The Independent claims are Claims 1, 42, 51, and 56. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Claim Rejections under 35 U.S.C. § 103(a)

The Examiner rejected Claims 1-9, 11-50, and 56-65 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,298,445 to Shostack, et al. (hereinafter the "Shostack" reference), and further in view of U.S. Patent No. 6,453,345 to Trcka, et al. (hereinafter the "Trcka" reference). Furthermore, the Examiner rejected Claims 51-55 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,070,190 to Reps, et al. (hereinafter the "Reps" reference), and further in view of the Shostack reference. The Applicants respectfully offer remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Shostack and Trcka references fail to describe, teach, or suggest the combination of (1) recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information; (4) displaying the one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; (5) receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat

procedure; (6) executing the selected one or more steps of the computer security threat procedure; (7) in response to executing the one or more steps of the selected procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date and time stamp; and (8) storing a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of the user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp, as recited in amended Claim 1.

The Shostack Reference

The Shostack reference describes a system that automatically provides software enhancements with updated information regarding security vulnerabilities. With the system of the Shostack reference, an enhancement is received from the network and integrated into the computer security software. Before the integration, a computer check can be performed to determine the integrity and the authenticity of the enhancement. The computer check can use cryptographic techniques such as digital signatures and Pretty Good Privacy (PGP) encryption. Shostack reference, column 2, lines 30-48.

The integrated system 160 of the Shostack reference includes a database 92 of security vulnerabilities that provides a secure operating environment. A first module 74 accesses the database 92 and assesses security vulnerabilities of an operating system of a computer. A second module 76 accesses the database and assesses security vulnerabilities of a computer network that includes the computer. A third module 78 accesses the database and assesses security vulnerabilities in passwords used to access the computer or the network. A fourth module 88 accesses the database and assesses security vulnerabilities of a remote computer connected to the network. A fifth module 90 receives an update to the database and updates the database. A sixth module is a communications module that allows communication between the integrated security system and a similar system. See Figure 5 below that illustrates the aforementioned modules of the integrated system 160. Shostack reference, column 11, line 61 through column 12, line 14.

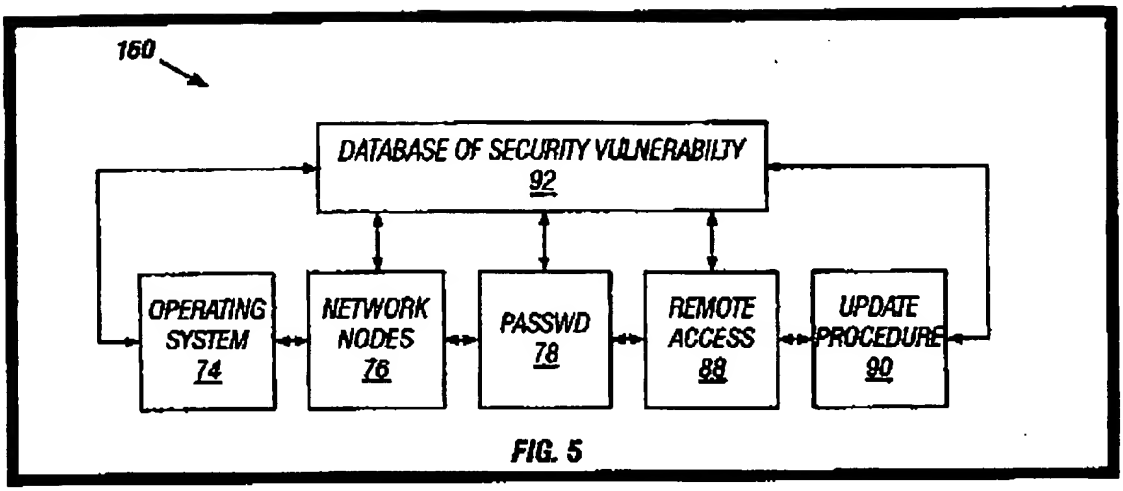

FIG. 5

The Shostack reference explains that the aforementioned and above illustrated modules of the integrated system are represented by corresponding symbols on a graphical user interface (GUI) screen 70 that is illustrated in Figure 6 below.

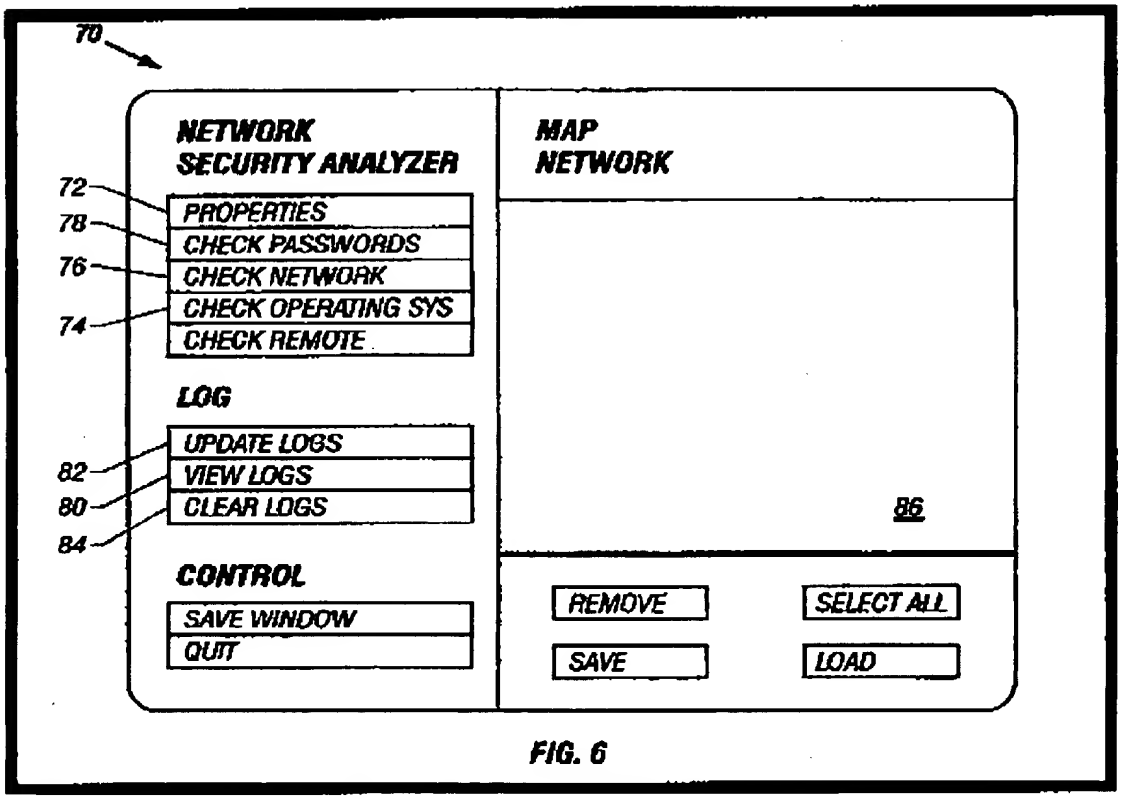

FIG. 6

The Shostack reference explains that the GUI 70 as illustrated in Figure 6 above provides a reporting mechanism. The GUI 70 includes several means for reporting various network transactions. The GUI 70 includes a log view 80 that may allow a user to view a text version of an update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log.

As noted above, the Examiner relies upon the Shostack reference to provide an alleged teaching of displaying one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; and receiving a selection of a suggested computer security threat procedure, the selection comprising one or more steps of the selected computer security threat procedure. However, the GUI 70 of the Shostack reference does not provide any teaching of displaying the procedure(s) and step(s) or for receiving a selection of a procedure and step(s).

For responding to security vulnerabilities, Shostack provides that "The update processor 54 also includes solutions for repairing the newly discovered vulnerabilities. The update processor 54 may automatically implement the suggested repairs of the system vulnerabilities and may send a message that the update is completed (Step 122)." Shostack reference, column 11, lines 50-54. Therefore, in the system of Shostack, after a software enhancement is received, the suggested repairs of the system vulnerabilities are implemented without allowing for the display of one or more suggested computer security threat procedures or the selection of a suggested computer security threat procedure, the selection comprising one or more steps of the selected computer security threat procedure.

The Examiner further relies upon the Shostack reference to provide an alleged teaching of storing a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of a user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp. However, the Shostack reference does not provide a teaching of the storage of this type of information. The Shostack reference merely provides for the storage of the software enhancement that is received

and a log of the software enhancement update. See e.g., Shostack reference, column 11, line 41; column 13, line 17.

The Trcka Reference

Furthermore, Applicants respectfully submit that Trcka reference fails to correct the deficiencies of the Shostack reference. The Examiner cited Trcka only for teaching of a date and time stamp. Applicants submit that the Trcka reference does not disclose the features discussed above.

In light of the differences between amended Claim 1 and the Shostack and Trcka references, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 42

The rejection of Claim 42 is respectfully traversed. It is respectfully submitted that the Shostack and Trcka references, fail to describe, teach, or suggest the combination of (1) classifying the computer security incident information; (2) automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information; (3) displaying the one or more computer security threat investigation procedures for investigating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (4) displaying one or more computer security threat response procedures for responding to one of suspicious computer activity comprising on or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (5) in response to a selection of a computer security investigation procedure, displaying one or more corresponding investigation steps; (6) in response to a selection of a computer security response procedure, displaying one or more corresponding response steps; (7) receiving a selection of one or more investigation steps and one or more corresponding response steps; and (8) storing a permanent record comprising computer security

incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps, as recited in amended Claim 42.

As noted above with respect to independent Claim 1, neither the Shostack reference nor the Trcka reference relate in any way to displaying the one or more computer security threat investigation procedures and response procedures or for receiving a selection of a computer security threat investigation procedure; computer security threat response procedure; and the corresponding steps of a computer security threat investigation procedure and response procedure; as recited in amended Claim 42. Furthermore, neither the Shostack reference nor the Trcka reference provide any teaching of storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps; as recited in amended Claim 42.

In light of the differences between Claim 42 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 42. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 51

The rejection of Claim 51 is respectfully traversed. It is respectfully submitted that the Reps and Shostack references, fail to describe, teach, or suggest the combination of (1) accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations, (2) the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, (3) the computer locations identifying devices that are able to perform computer security threat procedure associated with the computer security step information; (4) comparing a computer security threat procedure to be executed and a target Internet address with computer locations and Internet address ranges listed in the table; (5) determining if a match exists between an Internet address of a computer security incident and the Internet address ranges listed in the table; (6) automatically selecting a computer to execute the computer security threat

procedure based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident; and (7) storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps, as recited in amended Claim 51.

The Reps Reference

The Reps reference describes technology that is in the field of network system service, and particularly to an end-user based application availability and response monitoring and alerting system. The technology described by the Reps reference enables the monitoring of availability of response time or other desired performance metrics of an application program from the perspective of an end-user utilizing an application program over a distributed computing network. See the Reps reference, column 1, lines 24-31.

The Reps reference explains that a server computer 202 having an application program 203 provides application services to a client computer system 106 in which the client computer system 106 records information related to the performance of the services of the application program 203 via an application probe software 201 residing on the client computer system 1-6. See Figure 2 reproduced below and in column 5, lines 17-22 of the Reps reference.

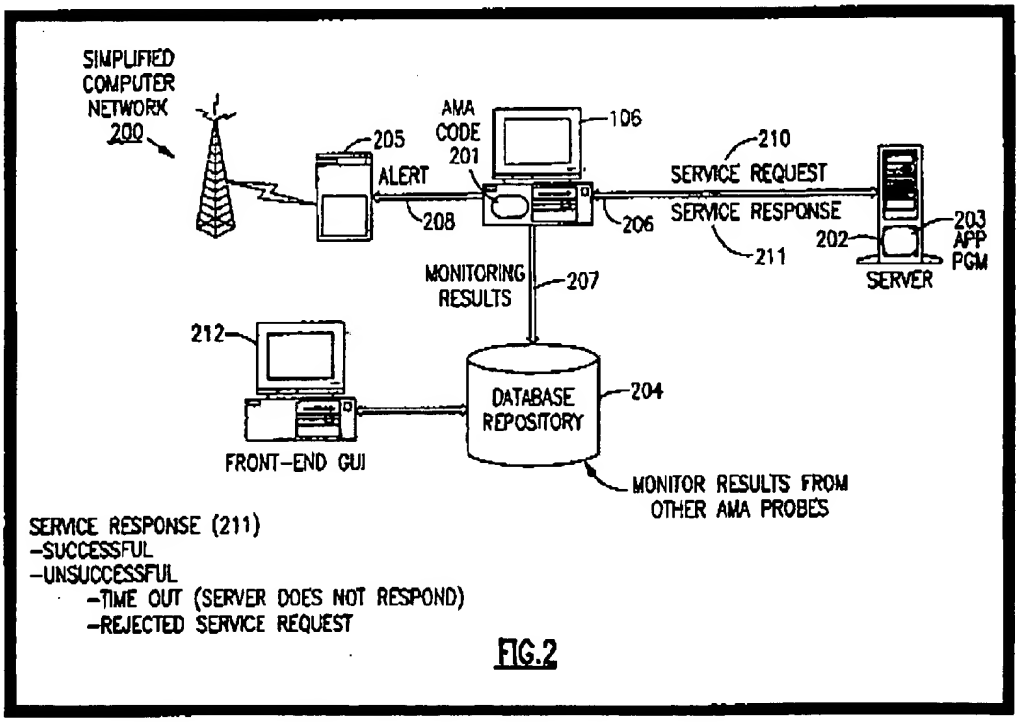

FIG.2

Specifically, as illustrated in Figure 2 above, an application monitoring alerting (AMA) probe 201 can establish a session with a server computer 202 by requesting the services of an application program 203 operating on the server computer 202 through a service request 210. The server computer's application program 203 provides a service response 211 over a network link 206 back to the requesting AMA probe 201. See the Reps reference, column 9, lines 58-68.

As noted in Figure 2, there are three types of service responses 211 transmitted back to the requesting AMA probe 201 from the server computer 202. First, if the application program 203 on the server computer 202 properly responds to the service request, the AMA probe 201 will receive an indication of a successfully completed request i.e., a successful service response, from the server computer 202. Secondly, if the server computer 202 is unavailable to respond to the service request 210, the request will timeout after a predetermined period and the AMA probe 201 will record that the server computer was not available, and indicate this as an unsuccessful service response. Finally, if the server computer 202 rejects the service request 210, the AMA probe will again record the transaction as an unsuccessful service response 211. See the Reps reference, column 10, lines 29-45.

Whether it is successful or unsuccessful, the service response 211 from the application program 203 on the server computer 202 (including the determination of a no-response time-out) is received at the AMA probe 201, which then records the results of the transaction in a database repository 204. See the Reps reference, column 10, lines 52-57.

The Reps reference does not provide any teaching of a computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat and executing a computer security threat procedure. Instead of a computer security threat, the Reps reference is primarily concerned with the level of service and performance of an application program 203 residing on a server 202. The Reps reference merely records the response 211 from the application program 203, whether the service request 210 was successful or unsuccessful. The Reps reference is not concerned with <u>why</u> a service request 210 may not have been successful.

The Reps and Shostack references also do not teach accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and

computer security threat procedure associated with the computer locations, the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, and the computer locations identifying devices that are able to perform the computer security threat procedure associated with the computer security step information, as recited in independent Claim 51.

To support the Examiner's finding that the Reps reference teaches some aspects of accessing a table comprising computer locations for one of investigating and responding to one of suspicious computer activity, the Examiner directs the Applicants' attention to Column 5, lines 46-48 and Column 11, lines 51-52 of the Reps reference.

> "In an embodiment of the invention these parameters may include such information as the name of the application program, the address of the server system..." Reps reference, column 5, lines 46-48.
>
> "[T]he probe configuration information 302 will include...the network address of the target server and the type of application on the target server to be monitored...." Reps reference, column 11, lines 48-53.

However, these passages only discuss storing location information to access the application server of the Reps reference. The application server of the Reps reference is not a computer location that is able to perform computer security steps associated with the computer security step information for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, as recited in amended independent Claim 51.

Furthermore, as noted above with respect to independent Claim 1, neither the Reps reference nor the Shostack reference provides any teaching of storing a permanent record comprising the executed computer security threat procedure and result information, and corresponding date and time stamps, as recited in amended independent Claim 51.

In light of the differences between Claim 51 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot

anticipate or render obvious the recitations as set forth in amended independent Claim 51. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 56

The rejection of Claim 56 is respectfully traversed. It is respectfully submitted that the Shostack and Trcka references, fail to describe, teach, or suggest the combination of (1) receiving computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) displaying one or more tools for one of investigating and responding to computer security incident information; (4) automatically suggesting one or more tools based on a classification of the computer security incident information; (5) receiving a selection of a suggested tool; (6) in response to a selection of a tool, forwarding data for execution of the tool; and (7) forwarding data for storing a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps, as recited in amended Claim 56.

As noted above with respect to independent Claim 1, neither the Shostack reference nor the Trcka reference relate in any way to displaying the one or more computer security threat investigation procedures and response procedures or for receiving a selection of a computer security threat investigation procedure; computer security threat response procedure; and the corresponding steps of a computer security threat investigation procedure and response procedure; as recited in amended Claim 56. Furthermore, neither the Shostack reference nor the Trcka reference provide any teaching of storing a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps; as recited in amended Claim 56.

In light of the differences between Claim 56 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 56. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicants also respectfully submit that the recitations of dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65 are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the remaining dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on September 7, 2006. The Applicants and the undersigned thank Examiner Ha for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-9 and 11-65. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.4647.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Reg. No. 54,004

King & Spalding LLP
34th Floor
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
404.572.4600
K&S Docket: 05456.105008